3

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/856,283	07/24/2001	Lyal Sidney Collins	U-013471-0	6730

7590 01/04/2005

LADAS & PARRY
224 SOUTH MICHIGAN AVENUE
CHICAGO, IL 60604

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Applicati n No.** 09/856,283	**Applicant(s)** COLLINS, LYAL SIDNEY	
	Examin r Shewaye Gelagay	**Art Unit** 2133	

-- The MAILING DATE of this communication appears n the cover sheet with the c rresp ndence address --

Period f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *July 24, 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *8/06&12/19/01; 2/14*/02

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been examined.

Claim Objections

2. Claim 2 is objected to because of the following informalities: the letter "a" in line 4 should be changed to the word "an". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 4, 7 and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Mapson WO 98/32260.

As per claim 4:

Mapson teach a method for reception of a securely transmitted message by a recipient device the method comprising the steps of:

(i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message; (Page 2, lines 9-11; receiving means is enabled to decrypt the message using first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with first identifiers)

(j) generating by a first process using the device identifier, the application identifier and the application value a message value; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc.; *The office has interpreted application value as an advanced transaction number: The interpretation is given based on the definition of the application value given on the disclosure*)

(k) generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; (Page 2, lines 26-30; the receiving means stores decryption information associated with the transmitting means ... this provides a unique key for each message without necessity for a real time link)

(l) combining the message value with the one or more secret values, to establish a secret message value; (Page7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(m) extracting a secure message block from the secure message; and (Page 2, lines 12-13; ...said message block is recognized as valid...)

(n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28; the receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number message can be decrypted)

As per claim 7:

Mapson teach an apparatus for reception of a securely transmitted message by a recipient device the apparatus comprising:

(i) extraction means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message; (Page 2, lines 9-11; receiving means is enabled to decrypt the message using first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with first identifiers)

(j) message generation means for generating, by a first process using the device identifier, the application identifier and the application value, a message value; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc.)

(k) secret value generating means for generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; (Page 2, lines 26-30; the receiving means stores decryption information associated with the transmitting means ... this provides a unique key for each message without necessity for a real time link)

(l) message value combining means for combining the message value with the one or more secret values, to establish a secret message value; (Page7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(m) secure message extraction means for extracting a secure message block from the secure message; (Page 2, lines 12-13; ...said message block is recognized as valid...) and

(n) application means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28; the receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number message can be decrypted)

As per claim 10:

Mapson teach a computer program product including a computer readable medium having recorded thereon a computer program for reception of a securely transmitted message by a recipient device the program comprising:

(i) extraction steps for extracting one or more of a device identifier, an application identifier and an application value from a received secure message; (Page 2, lines 9-11; receiving means is enabled to decrypt the message using first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with first identifiers)

(j) message generation steps for generating, by a first process using the device identifier, the application identifier and the application value, a message value; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc.)

(k) secret value generating steps for generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; (Page 2, lines 26-30; the receiving means stores decryption information associated with the transmitting means ... this provides a unique key for each message without necessity for a real time link)

(l) message value combining steps for combining the message value with the one or more secret values, to establish a secret message value; (Page7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(m) secure message extraction steps for extracting a secure message block from the secure message; (Page 2, lines 12-13; ...said message block is recognized as valid...) and

(n) application steps for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28; the receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number message can be decrypted)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-3, 5-6, 8-9 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mapson WO 98/32260 in view of Nixon et al. United States Letter Patent Number 5,828,851.

As per claim 1:

Mapson teach a method for encoding and transmitting by an originating device of a secure message the method comprising the steps of:

(a) generating by a first process using a device identifier, an application identifier and an application value a message value; (page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc)

(b) combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; (Page 7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(c) applying the secret message value and the message to an encoding process to form a secure message block; and (Page 2, lines 6-7; transmitting means encrypts said message; Page 5, lines 25-28; the secure device is capable of PIN encryption with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 1024 bit modulus Secure Device Issuer public key half.)

Mapson does not explicitly disclose

(d) combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

Nixon et al. in analogous art, however disclose combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value. (Col.10, lines 65-67 and Col. 11, line 2)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mapson to include combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Nixon et al. (Col. 2, lines 8-9) in order to have a control system that controls both devices that are defined using a standard protocol and other. This way, the source and destination address is combined to each message despite the type of network protocol they use to communicate.

As per claim 2:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson teach a method whereby an association of the device identifier, the application identifier, and the application value substantially uniquely identifies the originating device and a purpose of one or more of the message and the application, and a identifier for the message, such message identification being bound with the message content by virtue of the encoding process. (Page 2, lines 22-24; the encryption engine generates a unique key for each transaction, by operating a suitable function on one or more random or pseudo-random numbers generated by the transmitting means)

As per claim 3:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson teach a method whereby the encoding process in step (c) comprises one or more of:

(e) a symmetric encryption process; (Page 5, lines 25-26; the secure device is capable of PIN encryption with symmetric double length keys)

(f) an integrity process using one of keyed hash and symmetric encryption techniques; (Page 11, lines 1-6)

(g) a process including both symmetric encryption and keyed integrity; and

(h) including the secret message value in a higher level messaging protocol.

As per claim 5:

Mapson disclose an apparatus for encoding and transmitting by an originating device of a secure message, the apparatus comprising:

(a) message generating means for generating, by a first process using a device identifier, an application identifier and an application value a message value; (page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc)

(b) first combining means for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; (Page 7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(c) application means for applying the secret message value and the message to an encoding process to form a secure message block; (Page 2, lines 6-7; transmitting means encrypts said message; Page 5, lines 25-28; the secure device is capable of PIN encryption with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 1024 bit modulus Secure Device Issuer public key half.) and

Mapson does not explicitly disclose

(d) combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

Nixon et al. in analogous art, however disclose combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value. (Col.3, lines 48-55)

The rationale for combining the two references is the same as in claim 1.

As per claim 6:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson disclose an apparatus wherein the encoding means comprises one or more of:

(e) a symmetric encryption means; (Page 5, lines 25-26; the secure device is capable of PIN encryption with symmetric double length keys)

(f) an integrity processing means using keyed hash and symmetric encryption techniques; (Page 11, lines 1-6)

(g) a keyed-symmetric processing means performing symmetric encryption and keyed integrity; and

(h) encapsulation means for including the secret message value in a higher level messaging protocol.

As per claim 8:

Mapson disclose a computer program product including a computer readable medium having recorded thereon a computer program for encoding and transmitting by an originating device of a secure message, the program comprising:

(a) message generating steps for generating, by a first process using a device identifier, an application identifier and an application value a message value; (page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc)

(b) first combining steps for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; (Page 7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(c) application steps for applying the secret message value and the message to an encoding process to form a secure message block; (Page 2, lines 6-7; transmitting means encrypts said message; Page 5, lines 25-28; the secure device is capable of PIN encryption with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 1024 bit modulus Secure Device Issuer public key half.) and

Mapson does not explicitly disclose

(d) combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

Nixon et al. in analogous art, however disclose combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value. (Col.3, lines 48-55)

The rationale for combining the two references is the same as in claim 1.

As per claim 9:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson disclose a computer program product whereby the encoding steps in step (c) comprise one or more of:

(e) a symmetric encryption steps; (Page 5, lines 25-26; the secure device is capable of PIN encryption with symmetric double length keys)

(f) an integrity processing steps using one of keyed hash and symmetric encryption techniques; (Page 11, lines 1-6)

(g) keyed-symmetric steps performing symmetric encryption and ensuring keyed integrity; and

(h) encapsulation steps for including the secret message value in a higher level messaging protocol.

As per claim 11:

Mapson teach a system providing secure communications comprising an originating device and one or more receiving devices, wherein said originating device comprises an apparatus for encoding and transmitting a secure message, the originating device comprising:

(a) message generating means for generating, by a first process using a device identifier, an application identifier and an application value a message value; (page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc)

(b) first combining means for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; (Page 7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(c) application means for applying the secret message value and the message to an encoding process to form a secure message block; (Page 2, lines 6-7; transmitting means encrypts said message; Page 5, lines 25-28; the secure device is capable of PIN encryption with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 1024 bit modulus Secure Device Issuer public key half.) and

and wherein a said receiving device comprises an apparatus for reception of a securely transmitted message, said receiving device comprising:

(e) extraction means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message; (Page 2, lines 9-11; receiving means is enabled to decrypt the message using first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with first identifiers)

(f) message generation means for generating, by a first process using the device identifier, the application identifier and the application value, a message value; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc.)

(g) secret value generating means for generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; (Page 2, lines 26-30; the receiving means stores decryption information associated with the transmitting means ... this provides a unique key for each message without necessity for a real time link)

(h) message value combining means for combining the message value with the one or more secret values, to establish a secret message value; (Page7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(i) secure message extraction means for extracting a secure message block from the secure message; (Page 2, lines 12-13; ...said message block is recognized as valid...) and

(j) application means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28; the receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number message can be decrypted)

Mapson does not explicitly disclose

(d) combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

Nixon et al. in analogous art, however disclose combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value. (Col.3, lines 48-55)

The rationale for combining the two references is the same as in claim 1.

As per claim 12:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson further disclose a system;

wherein said originating device comprises:

(k) first processing means; (Page 2, lines 6-7)

(l) transmitting means adapted to perform one or more of establishing and maintaining communications with a receiving means, said first processing means being adapted to control said transmitting means, and adapted to support features (a) to (d); (Page 2,lines 4-8)

wherein a said receiving device comprises:

(m) second processing means; (Page 2, lines 26-28) and

(n) the receiving means, being adapted to perform one or more of establishing and maintaining communications in conjunction with said transmitting means, said second processing means being adapted control said receiving means, and further adapted to support features (e) to (j). (Page 2, lines 9-14)

As per claim 13:

Mapson and Nixon et al. teach all the subject matter as discussed above. In addition, Mapson disclose a system wherein said originating device comprises one of:

(o) a PC comprising the transmitting means, a smart card reader, the first processing means being responsive to the smart card reader and adapted to control said transmitting means, said originating device further comprising a smart card adapted to interface with the smart card reader, said smart card having on board second processing means which in conjunction with said first processing means are adapted to support features (a) to (d); and (Page 4, lines 22-24)

(p) a mobile telephone, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(q) a set top box, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(r) a cable modem, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(s) a personal digital assistant, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d).

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
Examiner
Art Unit 2133

12/17/04

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100